Welcome! Please do the following

- Connect to `Big Koala` wifi network. Password is `putinattackhelicopter`
- If you're on linux, run `# apt-get install nmap`
  - You do not need to do this on Kali because it's already there
- If you're on windows, download the following: `bit.ly/2HPpZG0`

  `bit.ly/2m6f8vF`

0 = <zero>

Network Recon

By Derek Ogle and Stanley Mugo

Networks

IP Address

- Address of computer - Like a PO box number for packets
- Example: 192.168.1.1
- Can range from 0.0.0.0 - 255.255.255.255
- Each number is called an octet
- 4 Billion totals IPv4’s

Public and Private IP’s & NAT

- 4 Billion is not enough IP’s for all computers in the world
- Public and Private IP’s solve this issue
- LAN’s use Private IP’s
- Internet uses Public IP’s
- Gateway between them does NAT (Network Address Translation)

Public and Private IP’s & NAT

Private IP Ranges

192.168.0.0 - 192.168.255.255

172.16.0.0 - 172.31.255.255

10.0.0.0 - 10.255.255.255

Things in these IP ranges are on an internal network and not directly exposed to the internet

Public and Private IP’s & NAT

Public IP Ranges

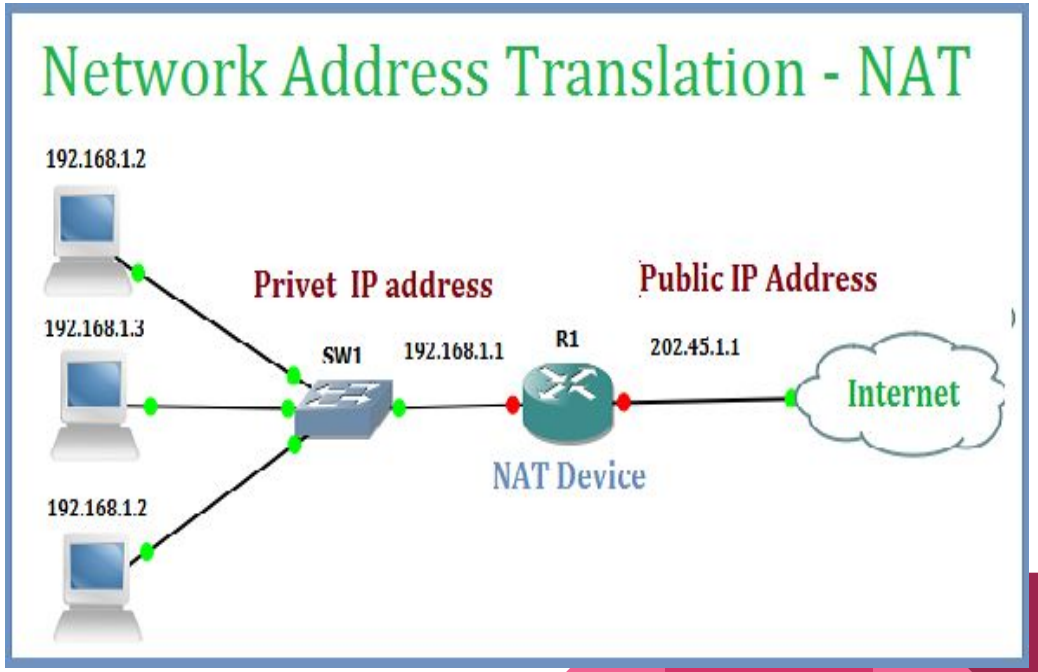
- Everything not in the last slide

Public IP’s will be directly accessible from the internet if not firewalled off

Public and Private IP’s & NAT

Network Address Translation

- Gateway that translates many private IP’s to one public
- Grayhats network is setup this way. 10.1.1.0/24 to 69.91.197.48
- Home networks are generally set up this way as well



Subnetting

- A subnet is some portion of the ip range
- Denoted using subnet notation. Ex. 192.168.1.0/24
- /x tells number of bits that stay the same from left to right
- /8 means first octet stays the same. Ex. 192.0.0.0/8
- /16 means first and second octet stay the same. Ex. 192.168.0.0/16
- /24 means the first three octets stay the same. 192.168.1.0/24
- Easier than specifying ip address ranges

Subnet Mask

- Used to determine which bits identify the subnet and which identify the host
- 255 means network and 0 means host
- For example 192.168.1.1 with a subnet mask of 255.255.255.0
- 192 168 1 1
  255 255 255 0

  N N N H

- The first 3 octets here identify the subnet and the last one identifies the host

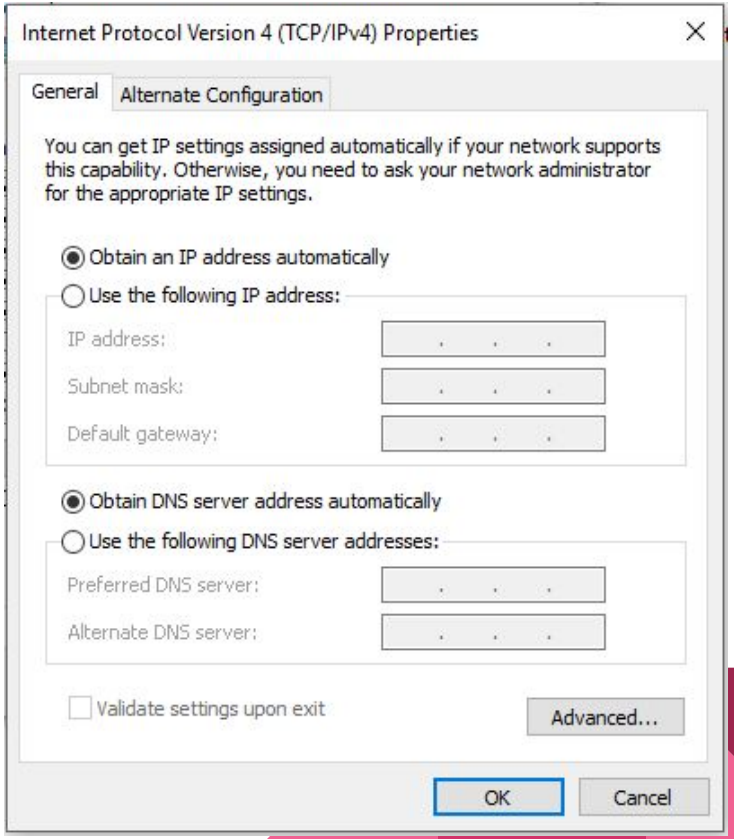
Subnet Behavior and Why

- Things on the same subnet can talk to each other
- Things on different subnets cannot talk unless a router is in place to let them
- Subnets are often used to isolate different types of devices
- For example, printers will often be on a different subnet than computers

Subnetting

Windows network config dialog showing the settings we just covered.

Default gateway is machine that does NAT. It's the way in and out of your subnet.



Ports

- An IP is like a PO box shared by many people
- Each person has a number and letters are addressed by IP and number
- This allows multiple communication channels from 1 IP address
- Port range is 0-65535
- Services generally run on a specific port

Ports

- Some examples are:
  - Telnet - 23
  - Remote Desktop - 3389
  - FTP - 20/21
  - SSH -22
  - HTTP - 80
  - HTTPS - 443
- These numbers aren’t guaranteed. For example Remote Desktop could run on port 6000 if it wanted
- Generally though port assignments are followed
- Most of the first 1000 ports are assigned to things

Addressing Ports

Connecting to a port is done using the following notation

Ip:portnumber

For example, 192.168.1.1:80 would connect to port 80 on 192.168.1.1

Port States

- Ports can have two states: Open and Closed
- Open ports are accepting connections
- Closed ports are not
- Port scanners look for open ports
- Ports who’s state cannot be determined are labeled as filtered
- Ports can be closed due to no service running or firewall rules

Hostnames / Domain Names

- The hostname is text thats mapped to an ip address
- Ex. google.com maps to 216.58.193.78
- Provides great info thats ip’s don’t
- Ex. MainServer1 is more helpful than 10.1.2.56

Services

Services

A service is software running on a host that talks over the network. We use recon to identify which services are running and which might be exploitable.

- Telnet / SSH / Mosh - remote shell access
- RDP / VNC - remote desktop access
- FTP / TFTP - file transfer
- HTTP[S] - web site transfer

SSH

SSH is a text based service. It essentially is a remote terminal allowing you to execute bash commands on the target computer

- Windows
  - putty
- Linux
  - ssh

Telnet

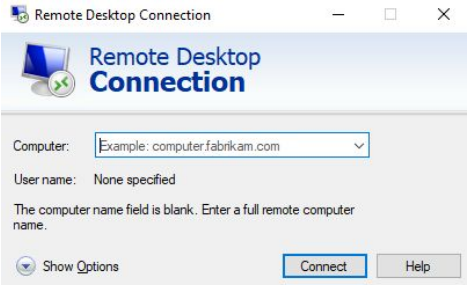
Telnet is like SSH but unencrypted. Operates similarly but unlike SSH is unencrypted

- Windows
  - putty
- Linux
  - telnet

Remote Desktop

Allows a remote user to interact with the computer as if they were sitting at it. Shows screen output and allow keyboard, mouse, and clipboard input.

- Windows
  - Builtin “Remote Desktop Connection”
- Linux
  - rdesktop



HTTP / HTTPS

The internet!

FTP

File transfer protocol. Allows uploading and downloading files from a remote machine. Often used to manage websites.

- Windows
  - putty
- Linux
  - ftp

VNC

Very similar to remote Desktop but not windows specific

Services

The point of recon is to identify these services and then gain access to them

Tools

Nslookup

- nslookup <ip>
  - nslookup type=mx <ip>

- for ((i = 67; i < 70; i++)); do nslookup “173.250.227.$i”; done

Nmap

- Most common scanning tool
- Allows scanning of ips, ip ranges, ports
- Offers service detection, version detection, OS fingerprinting
- Very versatile tool with dozens of features

Nmap Basic Usage

nmap <ip or hostname>

- Runs a basic port scan on the target
- Prints out a list of open ports and attempts to resolve the hostname
- Try this on 10.1.2.tbd

```
C:\Windows\system32>nmap 192.168.1.1

Starting Nmap 7.40 ( https://nmap.org ) at 2018-04-20 11:53 Pac
e
Nmap scan report for 192.168.1.1
Host is up (0.00s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    filtered ssh
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https
4567/tcp  filtered tram
8022/tcp  filtered oa-system
8080/tcp  open     http-proxy
8443/tcp  open     https-alt
MAC Address: C8:A7:0A:9E:BA:42 (Verizon Business)

Nmap done: 1 IP address (1 host up) scanned in 2.36 seconds

C:\Windows\system32>
```

Nmap and Pinging

- Nmap tries pinging the host in default mode
- Often times ping is disabled on the host
- Try nmap 10.1.2.tbd
- Now try with nmap -Pn 10.1.2.tbd
- -Pn means try port scanning without pinging first

Nmap and Fingerprinting

nmap -O <ip or hostname>

- -O tells nmap to attempt to guess the operating system
- It does this by looking at open ports and whats on them

Nmap and Fingerprinting

nmap -sV <ip or hostname>

- -A tells nmap to find version numbers

Nmap and Fingerprinting

nmap -A <ip or hostname>

- -A tells nmap to attempt to guess the operating system and anything else it can figure out
- Uses similar methods to -O but provides more info

Nmap and Ports

nmap -Pn <ip hostname> -p1-1000

Nmap taking forever

Increase/Decrease

- vV - verbosity
- dD - Debug
- pP - print route

Othertools

- netcat -raw sockets
- putty / ssh
- wireshark
- python

Recon tools

- nslookup <ip>
  - for ((i = 67; i < 70; i++)); do nslookup “173.250.227.$i”; done
- nmap <ip>
  - -sn
  - -Pn
  - -o
  - -sV
  - --spoof-mac
  - --badsum
- Post fingerprinting (Thought process to investigate)

Example